

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

Інв. № орг.	
Підп. та дата	
Взам. інв. №	
Інв. № дубл	
Підп. та дата	

Центр сертифікації ключів ринку електричної енергії

Комплексна система захисту інформації

Положення про службу захисту інформації

ЄААД.468244.185.П10

2014 р.

ЗМІСТ

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ	3
2 ЗАВДАННЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ	4
3 ФУНКЦІЇ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ	5
4 ПОВНОВАЖЕННЯ ТА ВІДПОВІДАЛЬНІСТЬ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ	7
5 ВЗАЄМОДІЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ З ІНШИМ ПЕРСОНАЛОМ ЦСК	10
6 ШТАТНИЙ РОЗКЛАД ТА СТРУКТУРА СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ	10
7 ОРГАНІЗАЦІЯ РОБІТ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ	10
8 ФІНАНСУВАННЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ	12

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 Положення є нормативним документом ДП "ЕНЕРГОРИНОК" і визначає завдання, функції, штатну структуру служби захисту інформації ЦСК (далі - СЗІ), повноваження та відповідальність співробітників СЗІ, взаємодію з іншими підрозділами організації та зовнішніми організаціями.

1.2 СЗІ складається з адміністраторів безпеки та керівника СЗІ, що призначаються з числа співробітників Департаменту інформаційних комп'ютерних систем наказом директора ДП "Енергоринок" та яким надаються повноваження щодо організації й впровадження технології захисту інформації, контролю стану захищеності інформації.

1.3 Метою створення СЗІ є організаційне забезпечення завдань керування комплексною системою захисту інформації (КСЗІ) у ЦСК та здійснення контролю за її функціонуванням. На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в ЦСК, проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації.

1.4 Правову основу для створення і діяльності СЗІ (що виконує функціональні обов'язки служби захисту інформації) становлять Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", "Положення про технічний захист інформації в Україні", НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі", Закон України "Про електронний цифровий підпис", наказ ДСТСЗІ СБУ від 13.01.2005 р. № 3 "Про затвердження Правил посиленої сертифікації", постанова Кабінету Міністрів від 13.06.2004 р. N 903 "Про затвердження Порядку акредитації центру сертифікації ключів"

1.5 СЗІ у своїй діяльності керується Конституцією України, законами України, нормативно-правовими актами Президента України і Кабінету Міністрів України, іншими нормативно-правовими актами з питань захисту інформації, державними і галузевими стандартами, розпорядчими та іншими документами організації, а також цим Положенням.

СЗІ здійснює діяльність відповідно до "Плану захисту інформації", календарних, перспективних та інших планів робіт, затверджених керівництвом ДП "ЕНЕРГОРИНОК" та ЦСК.

1.6 Для проведення окремих заходів з захисту інформації в автоматизованій системі ЦСК, наказом по ДП "ЕНЕРГОРИНОК" визначається перелік, строки виконання та відповідальні для виконання цих робіт.

1.7 У своїй роботі СЗІ взаємодіє з підрозділами ДП "ЕНЕРГОРИНОК", а також з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

У разі потреби, до виконання робіт можуть залучатися зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації.

2 ЗАВДАННЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

Завданнями СЗІ є:

- захист законних прав щодо безпеки інформації ДП "ЕНЕРГОРИНОК", окремих структурних підрозділів, персоналу в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах з зовнішніми вітчизняними організаціями;
- дослідження технології обробки інформації в ЦСК з метою виявлення можливих каналів витоку та інших загроз для безпеки інформації, формування моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;
- організація та координація робіт, пов'язаних з захистом інформації в ЦСК, необхідність захисту якої визначається її власником або чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;
- розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими повинен забезпечуватися захист інформації в ЦСК;
- організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу ЦСК;
- участь в організації професійної підготовки і підвищенні кваліфікації персоналу та абонентів ЦСК з питань захисту інформації;
- формування у персоналу і абонентів розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;
- організація забезпечення виконання персоналом і абонентами вимог нормативно-правових актів, нормативних і розпорядчих документів з захисту інформації в ЦСК та проведення контрольних перевірок їх виконання.

3 ФУНКЦІЇ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Функції під час створення комплексної системи захисту інформації

Основними функціями під час створення КСЗІ є:

- визначення переліків відомостей, які підлягають захисту в процесі обробки, інших об'єктів захисту в ЦСК, класифікація інформації за вимогами до її конфіденційності або важливості для ДП "ЕНЕРГОРИНОК", необхідних рівнів захищеності інформації, визначення порядку введення (виведення), використання та розпорядження інформації в ЦСК;
- розробка та коригування моделі загроз і моделі захисту інформації в ЦСК, політики безпеки інформації в ЦСК;
- визначення і формування вимог до КСЗІ;
- організація і координація робіт з проектування та розробки КСЗІ, безпосередня участь у проектних роботах зі створення КСЗІ;
- підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами та попередження спроб несанкціонованого доступу до інформації під час створення КСЗІ;
- організація робіт і участь у випробуваннях КСЗІ, проведенні її експертизи;
- вибір організацій-виконавців робіт зі створення КСЗІ, здійснення контролю за дотриманням встановленого порядку проведення робіт з захисту інформації, погодження основних технічних і розпорядчих документів, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проекти, програма і методика випробувань, плани робіт та ін.);
- участь у розробці нормативних документів, чинних у межах ДП "ЕНЕРГОРИНОК" і ЦСК, які встановлюють дисциплінарну відповідальність за порушення вимог з безпеки інформації та встановлених правил експлуатації КСЗІ;
- участь у розробці нормативних документів, чинних у межах ДП "ЕНЕРГОРИНОК" і ЦСК, які встановлюють правила доступу користувачів до ресурсів ЦСК, визначають порядок, норми, правила з захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій та ін.).

3.2 Функції під час експлуатації комплексної системи захисту інформації

Основними функціями під час експлуатації КСЗІ є:

- організація процесу керування КСЗІ;
- розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій;
- вжиття заходів у разі виявлення спроб НСД до ресурсів ЦСК, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;
- забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;
- організація керування доступом до ресурсів ЦСК (розподілення між користувачами необхідних реквізитів захисту інформації - паролів, привілеїв, ключів та ін.);
- супроводження і актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об'єктів, ідентифікатори користувачів тощо);
- спостереження (реєстрація і аудит подій в програмно-технічному комплексі ЦСК, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;
- підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в ЦСК, впровадження нових технологій захисту і модернізації КСЗІ;
- організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій в ЦСК або КСЗІ;
- участь у роботах з модернізації програмно-технічного комплексу ЦСК - узгодженні пропозицій з введення до його складу нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;

- забезпечення супроводження і актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;
- проведення аналітичної оцінки поточного стану безпеки інформації в ЦСК (прогнозування виникнення нових загроз і їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз та ін.);
- інформування абонентів ЦСК про технічні можливості захисту інформації в ЦСК і типові правила, встановлені для його персоналу і абонентів;
- негайне втручання в процес роботи програмно-технічного комплексу ЦСК у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;
- регулярне подання звітів керівнику ЦСК про виконання користувачами програмно-технічного комплексу ЦСК вимог з захисту інформації;
- аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання засобів для ЦСК ринку електричної енергії;
- контроль за виконанням персоналом і абонентами програмно-технічного комплексу ЦСК вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації;
- контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;
- розробка і реалізація комплексних заходів з безпеки інформації під час проведення нарад, переговорів та ін., здійснення їхнього технічного та інформаційного забезпечення.

3.3 Функції з організації навчання персоналу з питань забезпечення захисту інформації

Основними функціями з організації навчання персоналу є:

- розроблення планів навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу ЦСК;
- розроблення спеціальних програм навчання, які б враховували особливості технології обробки інформації в ЦСК, необхідний рівень її захищеності та ін.;
- участь в організації і проведенні навчання персоналу ЦСК правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;
- взаємодія з державними органами, учбовими закладами, іншими організаціями з питань навчання та підвищення кваліфікації;
- участь в організації забезпечення навчального процесу необхідною матеріальною базою, навчальними посібниками, нормативно-правовими актами, нормативними документами, методичною літературою та ін.

4 ПОВНОВАЖЕННЯ ТА ВІДПОВІДАЛЬНІСТЬ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Права

СЗІ має право:

- здійснювати контроль за діяльністю персоналу ЦСК щодо виконання ним вимог нормативно-правових актів і нормативних документів з захисту інформації;
- подавати керівництву ДП "ЕНЕРГОРИНОК" щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки тощо у випадку виявлення порушень політики безпеки або у випадку виникнення реальної загрози порушення безпеки;
- складати і подавати керівництву ДП "ЕНЕРГОРИНОК" акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їхнього усунення;
- проводити службові розслідування у випадках виявлення порушень;
- отримувати доступ до робіт та документів персоналу ЦСК, необхідних для оцінки вжитих заходів з захисту інформації та підготовки пропозицій щодо їхнього подальшого удосконалення;
- готувати пропозиції щодо залучення на договірній основі до виконання робіт з захисту інформації інших організацій, які мають ліцензії на відповідний вид діяльності;
- готувати пропозиції щодо забезпечення програмно-технічного комплексу ЦСК (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, які дозволені для використання в Україні з метою забезпечення захисту інформації;
- виходити до керівництва ДП "ЕНЕРГОРИНОК" з пропозиціями щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;
- узгоджувати умови включення до складу програмно-технічного комплексу ЦСК нових компонентів та подавати керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів;
- надавати висновки з питань, що належать до компетенції СЗІ, які необхідні для здійснення виробничої діяльності організації, особливо технологій, доступ до яких обмежено, інших проектів, що потребують технічної підтримки з боку співробітників СЗІ;
- виходити до керівництва ДП "ЕНЕРГОРИНОК" з пропозиціями щодо узгодження планів і регламенту відвідування програмно-технічного комплексу ЦСК сторонніми особами;
- інші права, які надані СЗІ у відповідності зі специфікою та особливостями діяльності ДП "ЕНЕРГОРИНОК".

4.2 Обов'язки

СЗІ зобов'язаний:

- організовувати забезпечення повноти та якісного виконання організаційно-технічних заходів з захисту інформації в ЦСК;
- вчасно і в повному обсязі доводити до персоналу ЦСК інформацію про зміни в галузі захисту інформації, які їх стосуються;
- перевіряти відповідність прийнятих в ЦСК правил, інструкцій щодо обробки інформації, здійснювати контроль за виконанням цих вимог;
- здійснювати контрольні перевірки стану захищеності інформації в ЦСК та подання звітів керівництву про результати перевірки;
- забезпечувати конфіденційність робіт з монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в програмно-технічному комплексі ЦСК;
- сприяти і, у разі необхідності, брати безпосередню участь у проведенні вищими органами перевірок стану захищеності інформації в програмно-технічному комплексі ЦСК;
- сприяти (технічними та організаційними заходами) створенню і дотриманню умов збереження інформації, отриманої ДП "ЕНЕРГОРИНОК" на договірних, контрактних або інших підставах від організацій-партнерів, постачальників, клієнтів, абонентів та приватних осіб;

- періодично, не рідше одного разу на місяць, подавати керівництву організації звіт про стан захищеності інформації в ЦСК і дотримання користувачами та персоналом ЦСК встановленого порядку і правил захисту інформації;
- негайно повідомляти керівництво ДП "ЕНЕРГОРИНОК" про виявлені атаки та викритих порушників;
- ведення журналу адміністратора безпеки у належному стані;
- не рідше одного разу на день перевірка цілісності конвертів з особистими ключами ЦСК та персоналу (основними та резервними) а також цілісності опечатування сейфів для зберігання особистих ключів і їх копій та іншої документації, у разі виявлення факту порушення упаковок або опечатування негайно доводити до відома керівництво ДП "ЕНЕРГОРИНОК";
- забезпечувати повноту та якісне виконання організаційно-технічних заходів із захисту інформації;
- розроблення розпорядчих документів, згідно з якими в ЦСК повинен забезпечуватися захист інформації, контроль за їх виконанням;
- своєчасно реагувати на спроби несанкціонованого доступу до ресурсів ЦСК, порушення правил експлуатації засобів захисту інформації;
- приймати участь у генерації ключів ЦСК та посадових осіб, формування для посадових осіб сертифікатів;
- приймати участь у знищенні особистого ключа ЦСК, контроль за правильним і своєчасним знищенням посадовими особами особистих ключів;
- контролювати процес резервування сертифікатів ключів та списків відкликаних сертифікатів, а також інших важливих ресурсів;
- організовувати розмежування доступу до ресурсів ЦСК, зокрема розподілення між посадовими особами паролів, ключів, сертифікатів тощо;
- забезпечувати спостереження (реєстрація та аудит подій в ЦСК, моніторинг подій тощо) за функціонуванням комплексної системи захисту інформації;
- забезпечувати організацію та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації після збоїв, відмов, аварій програмно-технічного комплексу ЦСК;
- подавати до центрального засвідчувального органу (засвідчувального центру) даних, необхідних для формування сертифіката та засвідчення відкритого ключа ЦСК;
- контролювати ведення журналів прийому-передачі ключів;
- забезпечувати використання особистого ключа ЦСК під час формування сертифікатів ключів, списків відкликаних сертифікатів та позначки часу;
- забезпечувати ведення, архівації та відновлення еталонної бази даних сформованих сертифікатів;
- інформування адміністратора безпеки про події, що впливають на безпеку функціонування ЦСК.
- перевіряти дані, обов'язкові для формування сертифіката, а також дані, які вносяться у сертифікат на вимогу підписувача;
- надавати допомогу підписувачам щодо вживання заходів із забезпечення безпеки інформації під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення;
- організовувати експлуатацію та технічне обслуговування комплексу засобів захисту (КЗЗ) програмно-технічного комплексу ЦСК;
- адмініструвати КЗЗ програмно-технічного комплексу ЦСК;
- приймати участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації;
- вести журнал аудиту подій, що реєструються засобами програмно-технічного комплексу ЦСК;
- встановлювати та налагоджувати програмне забезпечення системи резервного копіювання;
- формувати та вести резервні копії загальносистемного та спеціального програмного забезпечення ЦСК;
- забезпечувати актуальність еталонних, архівних і резервних копій баз сертифікатів, що створюються в ЦСК, та їх зберігання.

4.3 Відповідальність

4.3.1 Керівник СЗІ та співробітники СЗІ (адміністратор безпеки) за невиконання або неналежне виконання службових обов'язків, допущені ними порушення встановленого порядку захисту інформації в ЦСК несуть дисциплінарну, адміністративну, цивільно-правову, кримінальну відповідальність згідно з законодавством України.

Персональна відповідальність керівника СЗІ та співробітників СЗІ (адміністратора безпеки) визначається посадовими інструкціями.

4.3.2 Відповідальність за діяльність СЗІ покладається на її керівника.

4.3.2.1 Керівник СЗІ відповідає за:

- організацію робіт з захисту інформації в ЦСК, ефективність захисту інформації відповідно до діючих нормативно-правових актів;
- своєчасне розроблення і виконання "Плану захисту інформації";
- якісне виконання співробітниками СЗІ завдань, функцій та обов'язків, зазначених у цьому Положенні, посадових інструкціях, а також планових заходів з захисту інформації, затверджених керівництвом ДП "ЕНЕРГОРИНОК";
- координацію планів діяльності персоналу ЦСК ринку електричної енергії з питань захисту інформації;
- підготовку пропозицій щодо навчання персоналу ЦСК з питань захисту інформації;
- виконання особисто та співробітниками СЗІ розпоряджень керівника, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежної охорони.

4.3.2.2 Співробітники СЗІ (адміністратор безпеки) відповідають за:

- додержання вимог нормативних документів, що визначають порядок організації робіт з захисту інформації, інформаційних ресурсів та технологій;
- повноту та якість розроблення і впровадження організаційно-технічних заходів з захисту інформації в ЦСК, точність та достовірність отриманих результатів і висновків з питань, що належать до компетенції СЗІ;
- дотримання термінів проведення контрольних, інспекційних, перевірочних та інших заходів з оцінки стану захищеності інформації в ЦСК, які включені до плану робіт СЗІ;
- якість та правомірність документального оформлення результатів робіт окремих етапів створення КСЗІ, документального оформлення результатів перевірок;
- належне виконання своїх посадових обов'язків, правильність та повноту використання наданих прав, що передбачені їхніми посадовими інструкціями в межах визначених дійсним трудовим законодавством;
- порушення порядку дії в разі компрометації, виходу з ладу ключових носіїв інформації;
- залишення свого автоматизованого робочого місця без контролю, в тому числі в робочому стані;
- фіксування облікових записів користувачів (паролі, ідентифікатори, ключі та ін.) на неврахованих носіях, а також надання їх іншим особам окрім самого користувача;
- розголошення відомостей, що становлять комерційну таємницю та конфіденційних відомостей, які стали відомі по роду діяльності;
- правопорушення, які скоєні в процесі виконання своєї діяльності, - в межах визначених дійсним законодавством, кримінальним та цивільним законодавством;
- нанесення матеріального збитку - в межах, визначених дійсним трудовим та цивільним законодавством;
- своєчасне та належне виконання профілактичних, діагностичних та ремонтних робіт по усуненню несправностей на апаратурі програмно-технічного комплексу ЦСК;
- виконання норм експлуатації та забезпечення безперебійної роботи апаратури програмно-технічного комплексу ЦСК;
- невиконання правил безпеки при експлуатації ПЕОМ;
- за дотримання правил внутрішнього розпорядку, правил техніки безпеки, протипожежної безпеки, промислової санітарії та дотримання режиму безпеки інформації.

5 ВЗАЄМОДІЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ З ІНШИМ ПЕРСОНАЛОМ ЦСК

5.1 СЗІ здійснює свою діяльність у взаємодії з науковими, виробничими та іншими організаціями, державними органами і установами, що займаються питаннями захисту інформації.

5.2 Заходи з захисту інформації в ЦСК повинні бути узгоджені з заходами охоронної та режимної діяльності інших посадових осіб ДП "ЕНЕРГОРИНОК".

СЗІ взаємодіє, узгоджує свою діяльність та встановлює зв'язки з:

- зовнішніми організаціями, які є партнерами, користувачами, постачальниками, виконавцями робіт;
- іншими суб'єктами діяльності у сфері захисту інформації.

5.3 СЗІ координує свою діяльність з аудиторською службою під час проведення аудиторських перевірок.

5.4 Взаємодію з іншим персоналом ЦСК, що безпосередньо не пов'язані з захистом інформації, СЗІ здійснює у відповідності з наказами та (або) розпорядженнями керівництва ЦСК.

6 ШТАТНИЙ РОЗКЛАД ТА СТРУКТУРА СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

6.1 СЗІ безпосередньо підпорядкована керівнику ЦСК.

6.2 Структура СЗІ, її склад і чисельність визначаються фактичними потребами ЦСК для виконання вимог політики безпеки інформації та затверджуються керівництвом ДП "ЕНЕРГОРИНОК". Чисельність і склад СЗІ мають бути достатніми для виконання усіх завдань з захисту інформації в ЦСК.

6.3 Безпосереднє керівництво роботою СЗІ здійснює керівник СЗІ (Повноваження керівника СЗІ надаються співробітнику Департаменту інформаційних комп'ютерних систем наказом директора ДП "ЕНЕРГОРИНОК" або начальнику ЦСК). Призначення і звільнення з посади начальника СЗІ здійснюється керівництвом ДП "ЕНЕРГОРИНОК". На час відсутності начальника СЗІ (у зв'язку з відпусткою, службовим відрядженням, хворобою тощо) його обов'язки тимчасово виконує адміністратор безпеки (провідний спеціаліст з захисту інформації в комп'ютерних системах).

6.4 Штат СЗІ комплектується спеціалістами, які мають вищу спеціальну технічну освіту (у галузі ТЗІ або ІТ) та практичний досвід роботи, володіють навичками з розробки, впровадження, експлуатації КСЗІ і засобів захисту інформації, а також реалізації організаційних, технічних та інших заходів з захисту інформації, знаннями і вмінням застосовувати нормативно-правові документи у сфері захисту інформації.

6.5 Функціональні обов'язки співробітників визначаються переліком і характером завдань, які покладаються на СЗІ керівництвом ДП "ЕНЕРГОРИНОК".

6.6 Обов'язки адміністратора безпеки не можуть бути суміщені з іншими посадами.

6.7 Зміна структури СЗІ здійснюється за рішенням керівництва ДП "ЕНЕРГОРИНОК" і затверджується наказом (розпорядженням).

7 ОРГАНІЗАЦІЯ РОБІТ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

7.1 Трудові відносини в СЗІ будуються на основі законодавства України з урахуванням положень ДП "ЕНЕРГОРИНОК" правил внутрішнього трудового розпорядку та встановлених в ДП "ЕНЕРГОРИНОК" норм техніки безпеки праці, гігієни і санітарії, інших розпорядчих документів.

7.2 СЗІ здійснює свою роботу з реалізації основних організаційних та організаційно-технічних заходів зі створення і забезпечення функціонування КСЗІ у відповідності з планами робіт. Підставою для розроблення планів робіт є "План захисту інформації".

До планів включаються наступні основні заходи:

- разові (одноразово виконувані, необхідність у повторенні яких виникає за умови повного перегляду прийнятих рішень з захисту інформації);
- постійно виконувані (заходи, що потребують виконання неперервно або дискретно у випадковий чи заданий час);
- періодично виконувані (з заданим інтервалом часу);
- виконувані за необхідності (заходи, що потребують виконання під час здійснення або виникнення певних змін в програмно-технічному комплексі ЦСК чи зовнішньому середовищі).

Основними видами планів робіт СЗІ можуть бути:

- календарний план робіт (щодо реалізації заходів з проектування, реалізації, оцінювання, впровадження, технічного обслуговування, експлуатації КСЗІ та інших питань);
- план заходів з оперативного реагування на непередбачені ситуації (в тому числі надзвичайні та аварійні) та поновлення функціонування ЦСК;
- поточний план робіт (на місяць, квартал, рік);
- перспективний план розвитку та удосконалення діяльності СЗІ з питань захисту інформації (до 5 років);
- план заходів з забезпечення безпеки інформації під час виконання окремих важливих робіт, при проведенні нарад, укладенні договорів, угод тощо;
- бізнес-план створення і функціонування СЗІ.

Плани робіт складаються керівником СЗІ після обговорення на виробничій нараді СЗІ організаційно-технічних питань, що належать до її компетенції, і, за погодженням з начальником ЦСК, затверджуються керівництвом ДП "ЕНЕРГОРИНОК".

7.3 З метою забезпечення конфіденційності робіт, які виконуються співробітниками СЗІ, при прийомі на роботу (звільненні з роботи) вони дають письмові зобов'язання щодо нерозголошення відомостей, що становлять службову, комерційну або іншу таємницю, і які стали їм відомими в період роботи в організації.

7.4 Матеріально-технічну базу для забезпечення діяльності СЗІ складають належні йому на правах власності (оперативного управління, повного господарського відання) засоби захисту інформації, ПЗ, технічне і інженерне обладнання, засоби вимірювань і контролю, відповідна документація, а також інші засоби і обладнання, які необхідні для виконання СЗІ покладених на нього завдань.

Співробітники СЗІ відповідають за збереження майна, що є власністю або знаходиться у розпорядженні СЗІ.

Засоби захисту інформації та захищені засоби, що використовуються співробітниками СЗІ при виконанні своїх службових обов'язків, повинні мати, одержаний у встановленому порядку документ, що засвідчує їхню відповідність вимогам нормативних документів.

Матеріально-технічне та інше спеціальне забезпечення СЗІ здійснюється ДП "ЕНЕРГОРИНОК" у встановленому порядку.

8 ФІНАНСУВАННЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ

СЗІ фінансується за рахунок:

- коштів, що виділяються в організації на утримання органів управління;
- інших джерел фінансування, не заборонених законодавством.